Visory

CONSTRUCTION CYBER RISK GUIDE

Protect the projects, payments, people and momentum your business depends on.

Cyber risk shows up as business risk

Construction teams already manage tight schedules, changing conditions, dispersed jobsites and constant coordination. Cyber risk adds pressure when it interrupts payments, project information, communication or access to the systems people need to keep work moving.

This guide is designed to help leadership teams spot practical exposure, ask better questions and identify where stronger managed IT and security support can reduce disruption.

The goal is not more technology. It is fewer surprises, faster recovery and more confidence that the business can keep moving.

What is at risk?

Projects	Drawings, schedules, change orders and project records may become unavailable.
Payments	A compromised email or fraudulent request may redirect vendor or subcontractor funds.
People	Field and office employees may lose access to systems or wait for help during critical work.
Reputation	A missed commitment or exposed information can affect customers, partners and future opportunities.
Margin	Downtime, rework, recovery costs and diverted leadership attention can erode profitability.

Five risks worth discussing now



1. Payment and invoice fraud

A familiar-looking email can create an urgent request to change banking information, approve a wire or pay a revised invoice. The business impact is immediate: lost funds, delayed payments and strained vendor relationships.

PRACTICAL MOVE Require independent verification for banking changes, payment exceptions and urgent transfer requests.

2. Compromised email accounts

Email connects executives, accounting teams, vendors, subcontractors and customers. A compromised account can be used to observe conversations, impersonate trusted contacts or reset access to other systems.

PRACTICAL MOVE Use multifactor authentication, strong access controls and monitoring for unusual sign-in behavior.

3. Ransomware and system disruption

An attack can block access to files, email, ERP systems or project platforms. Even when data can be restored, the business may face downtime, recovery work and difficult customer conversations.

PRACTICAL MOVE Maintain protected backups, test recovery and define who leads the response.

4. Field devices and remote access

Laptops, tablets and phones move between homes, offices, jobsites and public networks. Lost devices, shared credentials and inconsistent security create gaps attackers can exploit.

PRACTICAL MOVE Manage every device consistently and remove access quickly when roles or employment change.

5. Vendor and subcontractor exposure

Construction depends on a broad network of partners. Shared files, portals, remote connections and email-based workflows mean another organization's weakness can become your problem.

PRACTICAL MOVE Limit third-party access, review it regularly and set clear security expectations.

Construction cyber risk checklist



Use this as a leadership conversation starter. Check each statement you can answer with confidence.

People and access

- [ ] Multifactor authentication is required for email, remote access and critical cloud applications.
- [ ] Employees receive practical training on phishing, payment fraud and suspicious requests.
- [ ] User access is added, changed and removed through a documented process.
- [ ] Administrative access is limited and reviewed.

Devices and jobsites

- [ ] Company laptops, tablets and phones are centrally managed.
- [ ] Security updates and endpoint protection are monitored across office and field devices.
- [ ] Lost or stolen devices can be locked or wiped.
- [ ] Jobsite and guest networks are separated from sensitive business systems.

Data and recovery

- [ ] Critical data is backed up and protected from the same credentials used in daily operations.
- [ ] Recovery is tested, not simply assumed.
- [ ] The team knows which systems must be restored first.
- [ ] Project files and sensitive records have clear access rules.



Email, payments and vendors

- [ ] Banking changes and unusual payment requests require verification through a second channel.
- [ ] Email security is monitored for impersonation, malicious links and suspicious activity.
- [ ] Third-party access is limited to what each partner needs.
- [ ] Vendor access is reviewed and removed when no longer required.

Response and accountability

- [ ] Leadership knows who owns incident response.
- [ ] Employees know how and where to report a suspicious event.
- [ ] The company has current contacts for IT, security, legal, insurance and communications support.
- [ ] An incident response exercise has been completed and lessons were documented.

If several answers are uncertain, that is useful information. It shows where focused improvements can reduce risk without turning security into another full-time job.

When something happens: the first response

A clear response protects time and reduces confusion. This is a business coordination framework, not a substitute for a formal incident response plan.

1

Report

Make it easy for employees to report suspicious emails, system behavior or payment requests immediately.

2

Contain

Disconnect affected devices or accounts from the environment without deleting information needed for investigation.

3

Coordinate

Bring together the designated IT/security lead, executive owner, insurer, counsel and communications resources as appropriate.

4

Protect payments

Notify financial teams and verify pending transactions if email or financial workflows may be affected.

5

Recover

Restore systems in the order the business has already defined and confirm they are safe before normal use resumes.

6

Learn

Document what happened, what worked and what should change.

IMPORTANT: If funds may have been redirected, contact the financial institution and authorities immediately. Preserve relevant emails, logs and device information.

What strong managed protection should feel like

The right MSP and security partner should reduce operational friction, not add another vendor to manage.

One accountable team	Clear ownership for support, security, remediation and escalation.
Security built into daily IT	Protection is part of how users, devices, email and systems are managed.
Support that understands urgency	Field and office employees can get help before a small issue slows the work.
Visibility for leadership	Risks, priorities and progress are explained in business terms.
A tested path forward	Recovery, response and modernization plans are documented before they are needed.

You do not need to solve every risk at once. Start by identifying what could stop the work, who owns the response and which gaps deserve attention first.

Your next conversation



A practical construction risk review should connect technology and security decisions to the business outcomes leadership already cares about:

Business outcomes

- **Project continuity**
- **Payment protection**
- **Employee productivity**
- **Customer and partner trust**
- **Cyber insurance and contract expectations**
- **Growth, acquisitions and new locations**

Questions to bring to the table

- Where would a technology disruption create the greatest operational impact?
- Which payment or vendor workflows depend most heavily on email?
- Who owns response and recovery if an incident occurs?
- How quickly could critical systems be restored?
- Are office, field and third-party access managed consistently?

VISORY | Managed IT + Security for construction firms

We protect what moves you forward.

Schedule a construction technology and security risk review with Visory.

www.visory.net